Canonical Valuations and the Birational Section Conjecture

K. J. Strømmen

August 31, 2015

Abstract

We develop a notion of a 'canonical $\mathcal{C}$-henselian valuation' for a class $\mathcal{C}$ of field extensions, generalizing the construction of the canonical henselian valuation of a field. We use this to show that the p-adic valuation on a finite extension F of $\mathbb{Q}_p$ can be recovered entirely (or up to some indeterminacy of the residue field) from various small quotients of G_F, the absolute Galois group of F. In particular, it can be recovered fully from the maximal solvable quotient. We use this to prove several versions of the birational section conjecture for varieties over p-adic fields.

1 Introduction

Let X/K be a complete, smooth and geometrically irreducible curve over a field K, with function field $F := K(X)$. Let $\hat{F}$ be any Galois extension, and put $\hat{K} := K \cap \hat{F}$. Then the canonical projection map of Galois groups $pr : Gal(\hat{F}/F) \to Gal(\hat{K}/K)$ sits in an exact sequence

$$1 \to Gal(\hat{F}/F\hat{K}) \to Gal(\hat{F}/F) \to Gal(\hat{K}/K) \to 1 \qquad (1)$$

2010 Mathematics Subject Classification. Primary 12J10, 11G25. Secondary 12E30

Keywords— Valuation theory, Galois groups, anabelian geometry, section conjecture, p-adic fields, rigid elements.

Given any $a \in X(K)$, we can assign to it a 'bouquet' of group-theoretic sections $s_a : Gal(\hat{K}/K) \to Gal(\hat{F}/F)$. Indeed, let v_a be the valuation on F corresponding to a, and w the valuation on $F\hat{K}$ corresponding to a preimage of a in $\hat{X} := X \otimes_K \hat{K}$ (so w extends v). If we let I_w and D_w denote the inertia and decomposition group of w/v inside $Gal(\hat{F}/F)$, then we get by Hilbert Decomposition Theory a commutative diagram

$$\begin{tikzcd}
1 \arrow[r] & Gal(\hat{F}/F\hat{K}) \arrow[r] & Gal(\hat{F}/F) \arrow[r, "pr"] & Gal(\hat{K}/K) \arrow[r] & 1 \\
1 \arrow[r] & I_w \arrow[r] \arrow[u] & D_w \arrow[r] \arrow[u] & G_w \arrow[r] \arrow[u, "\simeq"'] & 1
\end{tikzcd}$$

with exact rows. Here G_w denotes the Galois group of the residue field extension. It is known that the bottom row admits sections (see e.g. [8]). Any choice of such induces a section s_w of (4.1) such that $s(Gal(\hat{K}/K)) \subset D_w$, which is unique up to conjugation by an element of $Gal(\hat{F}/F\hat{K})$. Any member of the 'bouquet' of sections obtained in this manner is said to lie over a. In a similar manner, if v is a valuation which is trivial on K and has residue field K, the same discussion shows that v induces a 'bouquet' of sections which are said to lie over v. We call such valuations **K-valuations**

If we let $\mathcal{S}_{\hat{F}}$ denote the set of sections of (1) modulo conjugation, we have thus defined a map

$$\Psi_{\hat{F}} : X(K) \to \mathcal{S}_{\hat{F}}. \tag{2}$$

In particular, taking $\hat{F} = \overline{K(X)}$, this gives a map from $X(K)$ to sections of the exact sequence

$$1 \to G_{\overline{K}(X)} \to G_{K(X)} \to G_K \to 1, \tag{3}$$

where for any field F we let G_F denote its absolute Galois group. As part of his visionary programme of 'anabelian geometry', outlined in his famous "Esquisse d'un Programme" (see the appendix of [12]), Grothendieck made the following conjecture:

Birational Section Conjecture. (A. Grothendieck) *Let K be a field finitely generated over $\mathbb{Q}$ or a finite extension of $\mathbb{Q}_p$ for some prime p. Then*

$$\Psi_{\overline{K}} : X(K) \to \mathcal{S}_{\overline{K}}$$

is a bijection. In particular, the existence of a section of (3) implies the existence of a rational point on X.

In [6], Koenigsmann establishes the local version of this conjecture, i.e. the case where K is a finite extension of $\mathbb{Q}_p$. Later, Pop showed in [10] the even stronger result that $\Psi_{F''} : X(K) \to S_{F''}$ is a bijection, where F'' denotes the maximal elementary $\mathbb{Z}/p$ meta-abelian extension of F, with F a finite extension of $\mathbb{Q}_p$ containing a primitive p-th root of unity.[1]

In this note we aim to show a result somewhere in between, namely that one can take $\hat{F} = F^{solv}$, the maximal solvable extension of F:

Theorem 1.1. *Let K be a finite extension of $\mathbb{Q}_p$. If F^{solv} denotes the maximal solvable extension of F, then the map*

$$\Psi_{F^{solv}} : X(K) \to \mathcal{S}_{F^{solv}}$$

is a bijection.

This follows from Pop's Theorem in the case where K contains a primitive p-th root of unity. Pop's proof uses local-global principles for Brauer groups and uses crucially the fact that one is working with function fields of curves. The main novelty of this note is the method of proof, which goes instead via the following new group theoretic characterization of the existence of certain valuations on a field, of interest in its own right:

Theorem 1.2. *Let K be any field, p a prime. Then there is a valuation v on K, extending uniquely to K^{solv}, with $\Gamma_v \neq p\Gamma_v$ and $char(Kv) \neq p$ if and only if $Gal(K^{solv}/K)$ has a non-procyclic p-Sylow subgroup with a non-trivial abelian normal subgroup.*

To do this, we develop a general machinery of 'canonical valuations' which allow one to deduce the section conjecture for any $\hat{F}$ satisfying certain technical properties. Roughly speaking, if the choice of $\hat{F}$ is such that one can

[1] He proves a slightly weaker result in the case when F does not contain roots of unity which still implies Koenigsmann's original result.

develop a 'good' notion of a $\hat{F}$-henselian valuation (i.e. a valuation on F extending uniquely to $\hat{F}$), then we show that bijectivity of (2) is a purely formal consequence of the arguments from [4] and [1]. Theorem 1.2 then follows from the fact that F^{solv} satisfies the required properties.

In fact, pushing these arguments to their limit, we can even take $\hat{F}$ to be F^{pq}, the maximal (p, q)-meta-abelian extension of F, where p and q are two distinct primes and F is a p-adic field containing a primitive p-th and q-th root of unity.[2][3] The techniques here are based upon the fundamental characterization in [5]. With F as above, provided F contains ζ_l, where l is a prime not equal to p, then one can show that

$$G_F(l) \simeq \mathbb{Z}_l \rtimes \mathbb{Z}_l.$$

where $G_F(l)$ denotes the maximal pro-l quotient of G_F. In [5] it is shown that any field L with the same maximal pro-l quotient must admit a l-henselian valuation so-called tamely branching at l. Since l is arbitrary, it is clear that this criterion alone cannot recover a fully p-adic valuation. We will show that as soon as you add in some minimal knowledge of p-power extensions in the Galois group, you can recover it almost completely. In fact, we show that the maximal solvable quotient of the absolute Galois group recovers the valuation completely, while $Gal(F^{pq}/F)$, in the presence of roots of unity, recovers it up to some indeterminacy of the residue field. This gives a significant strengthening of the main result in [4].

Due to the strength of Theorem 1.2, we can also easily prove an analogue of the section conjecture for p-adic *varieties* as well (Theorem 10.1) in this paper), stating that sections correspond to unique K-valuations.

2 Preliminaries

2.1 Notation and Conventions

Let K be a valued field, with valuation v. Denote the valuation ring $\mathcal{O}_v$, the value group Γ_v and the residue field Kv. If $a \in \mathcal{O}_v$, denote by $\bar{a}$ the image of a in Kv. Given two valuation rings $\mathcal{O}_1$ and $\mathcal{O}_2$ on a field, $\mathcal{O}_2$ is said to be *coarser* than $\mathcal{O}_1$ if $\mathcal{O}_1 \subset \mathcal{O}_2$. Two valuations are called *comparable* if one is

[2] See Definition 8.6.

[3] Taking $\hat{F} = F^{pq}$ appears to be best possible using these methods, though see [7] for a strengthening when $F = \mathbb{Q}_2$.

coarser than the other.

Given a field K, let $G_K := Gal(K^{sep}/K)$ denote the Galois group of a fixed separable closure of K. We have the following two important subfields of K^{sep}:

- $K(p)$, the maximal p-power extension of K, p a prime. That is, the compositum of all extensions L/K with $[L:K] = p^n$ for some n.
- $K(p,q)$, the maximal (p,q)-extension of K, p and q distinct primes. That is, the compositum of all extensions L/K with $[L:K] = p^n q^m$ for some n, m.
- K^{solv}, the maximal solvable extension of K, i.e. the compositum of all extensions L/K with $Gal(L/K)$ solvable.

The Galois groups $Gal(K(p)/K)$, $Gal(K(p,q)/K)$ and $Gal(K^{solv}/K)$ are naturally quotients of G_K. We denote them by $G_K(p)$, $G_K(p,q)$ and G_K^{solv} respectively.

3 Some Galois Cohomology

We recall some basics on Galois cohomology and the connection with Brauer groups and norms. The aim of this is to establish that the surjectivity of certain norm maps is a Galois theoretic property encoded by a very small quotient of G_K.

Let p be a prime, G a pro-p group with rank n. Let $H^i(G) := H^i(G, \mathbb{Z}/p\mathbb{Z})$, $i \in \mathbb{N}$ be the i-th Galois cohomology group.

If K is a field and L/K is a finite Galois extension, we let $N_{L/K} : L^\times \to K^\times$ denote the norm map. When $L = K(\sqrt[p]{a})$ for some $a \in K^\times$, we let $N(a)$ denote the image $N_{L/K}(L^\times)$.

Now suppose $G = G_K(p)$, the maximal pro-p quotient of G_K, is finitely generated, where K is a field containing ζ_p, a primitive p-th root of unity. Then Kummer Theory provides an isomorphism

$$H^1(G_K(p), \mathbb{Z}/p\mathbb{Z}) \simeq K^\times/(K^\times)^p$$

and the theory of Brauer groups gives

$$H^2(G_K(p), \mathbb{Z}/p\mathbb{Z}) \simeq {}_pBr(K) \simeq (\mathbb{Z}/p\mathbb{Z})^n$$

for some $n < \infty$, where ${}_pBr(K)$ is the p-torsion subgroup of the Brauer group of K. The cup-product pairing can be identified with the Hilbert symbol

$$K^\times/(K^\times)^p \times K^\times/(K^\times)^p \to (\mathbb{Z}/p\mathbb{Z})^n$$

sending the pair a, b to the symbol $(a, b)_K$ corresponding to the central simple K-algebra with generators x, y subject to the relations $x^p = a, y^p = b, xy = \zeta_p yx$. We have $(a, b)_K = 1$ iff $a \in N(b)$ iff $b \in N(a)$.

We will want to make use of a strengthening of the above observation. To this end we first make the following definition:

Definition 3.1. Given a field K containing ζ_p, let K' denote the maximal $\mathbb{Z}/p\mathbb{Z}$ elementary abelian extension of K: thus $K' = K(\sqrt[p]{K^\times})$. Let K'' denote the maximal $\mathbb{Z}/p\mathbb{Z}$ elementary meta-abelian extension of K. That is, $K'' = (K')'$.

If $G = G_K(p)$, we let $G' := Gal(K'/K)$, $G'' := Gal(K''/K)$.

Proposition 3.2. *Let $G = G_K(p)$ where K is a field containing ζ_p. Then*

(i) $H^1(G) \simeq H^1(G') \simeq K^\times/(K^\times)^p$;

(ii) Given $a, b \in H^1(G)$, we have that $a \cup b = 0$ in $H^2(G)$ if and only if $a \cup b = 0$ in $H^2(G'')$.

In particular, given a, b in $K^\times/(K^\times)^p$, whether or not $(a, b)_K$ is 1 or -1 can be read off G''.

Proof. Part (i) is just Kummer theory. For part (ii), see [10], Lemma 1. □

We will also recall some basic facts about the cohomological dimension $cd(G)$ of a pro-p group G.

Proposition 3.3. *Let G be a pro-p group. Then*

(i) $cd(G) \leq n$ if and only if $H^{n+1}(G, \mathbb{Z}/p\mathbb{Z}) = 0$;

(ii) $cd(G) = 1$ if and only if G is a free pro-p group;

(iii) If $G = G_K(p)$, where K is a field containing ζ_p, then $cd(G) = 1$ if and only if for every $a \in K^\times \setminus (K^\times)^p$, the norm map

$$N_{L/F} : L^\times \to K^\times$$

is surjective, where $L = K(\sqrt[p]{a})$. Equivalently, ${}_pBr(K) = 0$.

Proof. The first two items are standard (see [13]). The last claim follows from the isomorphism $H^2(G_K(p), \mathbb{Z}/p\mathbb{Z}) \simeq {}_pBr(K)$ and the fact that ${}_pBr(K)$ is generated by the symbols $(a,b)_K$ (the Merkurjev-Suslin Theorem) which are trivial exactly when $b \in N(a)$. □

In fact, by Proposition 3.2, the conclusion of (iii) above holds even when G is taken to be G''.

3.1 Notions of Henselianity

Definition 3.4. Let H be a Galois extension of K, not necessarily finite. Then $(K, \mathcal{O})$ is called H-henselian if $\mathcal{O}$ extends uniquely to H. Equivalently, if $\mathcal{O}$ extends uniquely to every finite sub-extension $K \subset L \subset H$.

Lemma 3.5. *(Hensels Lemma) The following are equivalent:*

(i) v is H-henselian;

(ii) Let $f \in \mathcal{O}_v[x]$ be a polynomial which splits in H. Then for every $a \in \mathcal{O}_v$ with $\bar{f}(\bar{a}) = 0$ and $\bar{f}'(\bar{a}) \neq 0$, there exists $\alpha \in \mathcal{O}$ with $f(\alpha) = 0$ and $\bar{\alpha} = \bar{a}$.

(iii) Suppose the polynomial $x^n + x^{n-1} + a_{n-2}x^{n-2} + \ldots + a_0 \in \mathcal{O}_v[x]$, with $a_{n-2}, \ldots, a_0 \in \mathcal{M}_v$, splits in H. Then it has a zero in K.

Remark 3.6. Note that given any valued field (K, v), we can always find an H-henselization of it, that is, an extension (K^h, v^h) of valued fields such that v^h is H-henselian.

The following choices of H will be of crucial importance in the rest of this paper:

- $H = K^{sep}$. In this case we call an H-henselian valuation simply *henselian.*

- $H = K(p)$, the maximal p-power extension of K for some prime p (that is, the compositum of all Galois extensions of K of degree p^n for some n). In this case we call a H-henselian valuation *p-henselian.*

- $H = K$: the compositum of all Galois extensions of K of degree $p^n q^m$. We call this the maximal (p,q)-extension of K. In this case an H-henselian valuation is called (p,q)-henselian.

- $H = K^{solv}$: the maximal pro-solvable extension of K. In this case we call a H-henselian valuation *solv-henselian.*

In the case of p-henselianity we have the following useful observation (see [1], Theorem 4.2.2).

Lemma 3.7. *A valuation v on a field K is p-henselian if and only if it extends uniquely to every Galois extension of K of degree p.*

4 Canonical classes

Definition 4.1. Let $\mathcal{C}$ be a class of finite groups closed under extensions, subgroups and quotients. If G is a profinite group, we let G^c denote the maximal pro-$\mathcal{C}$ quotient of G. If $G = G_K$, we define K^c to be the unique subextension of K^{sep} with $G_K^c = Gal(K^c/K)$. For any field K, we let $\mathcal{C}(K)$ denote the set of Galois subextensions of K^c/K.

By Galois theory, the following properties are immediate:

(i) If $L, F \in \mathcal{C}(K)$ then the compositum $LF \in \mathcal{C}(K)$;

(ii) If $L \in \mathcal{C}(K)$ and F/K is a subfield of L, then $F \in \mathcal{C}(K)$;

(iii) If $L \in \mathcal{C}(K)$ and $M \in \mathcal{C}(L)$ then $M \in \mathcal{C}(K)$;

(iv) $(K^c)^c = K^c$.

From now on $\mathcal{C}$ will always refer to such a class.

Definition 4.2. A valuation on K which is K^c-henselian with respect to a class $\mathcal{C}$ is called $\mathcal{C}$-henselian or simply *c-henselian.* We also say that K is c-closed if $K = K^c$.

We have the following proto-typical examples:

- $\mathcal{C} = \mathcal{C}_{sep}$, the class of all finite groups. Then $K^c = K^{sep}$ and c-henselianity is the same as henselianity.

- $\mathcal{C} = \mathcal{C}_p$, the class of all p-groups. Then $K^c = K(p)$ and c-henselianity is the same as p-henselianity.

- $\mathcal{C} = \mathcal{C}_{solv}$, the class of all solvable finite groups. Then we write $K^c = K^{solv}$, and call a c-henselian valuation *solv-henselian.*

Definition 4.3. Let $\mathcal{C}_1$ and $\mathcal{C}_2$ be two classes. We say that $\mathcal{C}_1$ *contains* $\mathcal{C}_2$ if, for any profinite group G, G^{c_2} is obtained from G^{c_1} as the quotient by a characteristic subgroup. Note that in this case, the class of finite groups in $\mathcal{C}_1$ actually contains the finite groups in $\mathcal{C}_2$.

On the field-theory side, if $\mathcal{C}_1$ contains $\mathcal{C}_2$, then for any field K, if $L \in \mathcal{C}_2(K)$, also $L \in \mathcal{C}_1(K)$.

Example 4.4. We have that $\mathcal{C}_{solv}$ contains $\mathcal{C}_p$ for any p. Indeed, let G^p denote the maximal pro-p quotient, and G^s the maximal solvable quotient. Then G^p is the quotient of G^s by the normal subgroup generated by all its Sylow q subgroups, $q \neq p$, which is characteristic (since any automorphism sends a Sylow q-subgroup to another Sylow q-subgroup).

Since isomorphisms descend to quotients by characteristic subgroups, we get that if $\mathcal{C}_1$ contains $\mathcal{C}_2$, then

$$G_F^{c_1} \simeq G_K^{c_1} \Rightarrow G_F^{c_2} \simeq G_K^{c_2}$$

for any two fields F and K.

Definition 4.5. Call a class $\mathcal{C}$ *canonical* if the following conditions hold for any field K.

(L) Let v be a c-henselian valuation on K, and assume $K^c v/Kv$ is separable. Then $K^c v \in \mathcal{C}(Kv)$, and for any $L \in \mathcal{C}(Kv)$, there exists a (not necessarily unique) $L' \in \mathcal{C}(K)$ such that $L'w = L$, where w is the unique extension of v. In particular, if $K^c = K$ then $(Kv)^c = (K^c)v = Kv$.

(S) If $\mathcal{O}_1$ and $\mathcal{O}_2$ are two independent c-henselian valuations on a field K, then $K = K^c$.

(R) If K^c is a finite extension of K, then $[K^c : K] \leq 2$.

Note: From now on, when we refer to a class $\mathcal{C}$ it will always refer to a canonical class, and a c-henselian valuation will always be with respect to some canonical class $\mathcal{C}$.

As indicated (see [1] p.103 and [5]), we have the following known result:

Fact 4.6. *The classes $\mathcal{C}_{sep}$ and $\mathcal{C}_p$ are canonical.*

Remark 4.7. To explain condition (R), recall the following classical results: K is real-closed (resp. Euclidean) if and only if $\overline{K}$ (resp. $K(2)$) is a finite, non-trivial extension of K, and in this case, the extension is of degree 2. Therefore this condition will allow us to keep close control over the behaviour of K in the unusual cases where K^c is a finite extension of K.

The following simple observation is crucial:

Proposition 4.8. *Let $\mathcal{C}_{solv}$ be the class of solvable finite groups. Then $\mathcal{C}_{solv}$ is a canonical class.*

Proof. Since $\mathcal{C}_{solv}$ is closed under extensions, subgroups and quotients, it is a class in the sense of this paper. It remains to show that this class is canonical.

Suppose v is a solv-henselian valuation on a field K. We need to show that we can lift solvable Galois extensions of Kv to solvable Galois extensions of K. By Galois theory, the solvable Galois extensions are exactly the radical ones. Since v is solv-henselian, and every Galois extension of degree p is solvable, v is p-henselian for every prime p, by Lemma 3.7. Since $\mathcal{C}_p$ is canonical, any Galois extension of degree p of Kv can be lifted to K. Because any radical Galois extension can be written as a succession of extensions of prime degree, we can thus lift any radical Galois extension of Kv to K. Note that for a field of characteristic p, a radical extension of degree p is to be interpreted as an Artin-Schreier extension of degree p, i.e., an extension obtained by adjoining the roots of a polynomial of the form $x^p - x - a$. In the case when the valued field (K, v) is of mixed characteristic $(0, p)$, assuming $\zeta_p \in K$, then such extensions of the residue field become 'actual' radical extensions of K, namely the extension of degree p obtained by adjoining a p-th root of $1 + (\zeta_p - 1)^p a$. Hence $\mathcal{C}_{solv}$ satisfies property (L).

Next, suppose v_1 and v_2 are two independent solv-henselian valuations on a field K. As remarked in the above argument, v_1 and v_2 are in particular

p-henselian for every prime p. Since $\mathcal{C}_p$ is a canonical class, it follows that K does not admit any non-trivial extensions of degree p. Hence it does not admit any radical extensions, whence $K = K^c$, implying that $\mathcal{C}_{solv}$ satisfies property (S).

Finally, if $[K^c : K] < \infty$, then $[K(p) : K] < \infty$ for every prime p. Again using that $\mathcal{C}_p$ is canonical, we find that $K^c = K(2)$ and $[K(2) : K] \leq 2$. Hence $\mathcal{C}_{solv}$ satisfies (R). □

In an entirely analogous fashion we can prove the following:

Proposition 4.9. *Given two primes p, q, let $\mathcal{C}_{p,q}$ be the class of finite (p,q)-groups, i.e., groups of cardinality $p^n q^m$ for some n, m. Then $\mathcal{C}_{p,q}$ is a canonical class.*

We shall see that $\mathcal{C}$-henselian valuations with respect to a canonical class $\mathcal{C}$ admit a notion of a canonical c-henselian valuation. The first property we will need in this direction is that c-henselianity behaves well with respect to compositions of valuations. Indeed, let v_1 and v_2 be valuations on a field K with valuation rings $\mathcal{O}_1$ and $\mathcal{O}_2$ respectively. If $\mathcal{O}_1 \subset \mathcal{O}_2$, so v_2 is a coarsening of v_1, we get an 'exact sequence of valuations

$$1 \to v_2 \to v_1 \to v_1/v_2 \to 1 \tag{4}$$

Here v_2/v_1 is the induced valuation on Kv_2 with valuation ring $\overline{\mathcal{O}_1} := \mathcal{O}_1/\mathcal{M}_2$ and maximal ideal $\overline{\mathcal{M}_1} := \mathcal{M}_1/\mathcal{M}_2$. The 'lifting' property (L) is the key to the following

Lemma 4.10. *Given an exact sequence of valuations as above, then v_1 is c-henselian if and only if v_2 and v_1/v_2 is.*

Proof. Suppose v_1 is c-henselian. Let

$$f = x^n + x^{n-1} + a_{n-2}x^{n-2} + \ldots + a_0 \in O_2[x]$$

be such that $a_i \in \mathcal{M}_1$. If f splits in K^c then since $\mathcal{M}_2 \subset \mathcal{M}_1$, Lemma 3.5 implies that f has a zero in K and so v_2 is c-henselian. Next, assume that $\bar{a_i} \in \mathcal{M}_1/\mathcal{M}_2$, and suppose $\bar{f}$ splits in $Kv_1^c = (K^c)v_1$. We may assume that f splits in K^c. Indeed, without loss of generality suppose f is irreducible. If $\bar{f}(\alpha) = 0$ for $\alpha \in (Kv)^c$, then by property (L), there is an extension $F \in \mathcal{C}(K)$ such that Fv is the splitting field of $\bar{f}$. Then we can simply replace f by the minimal polynomial of $a \in F$ with $\bar{a} = \alpha$. Hence f has a zero in $\mathcal{O}_1$ by c-henselianity, and so also in Kv_1. Thus v_2 and v_1/v_2 are both c-henselian.

The other direction is straightforward. Let $f \in \mathcal{O}_1[x]$ be a polynomial which splits in K^c and has a root in Kv_1. Then using c-henselianity of first v_1/v_2 and then v_2 one lifts the root first to Hence $G_K^c = Gal(K^c/K)$. $\mathcal{O}_1/\mathcal{M}_1$ and then to K. □

5 Constructing the canonical c-henselian valuation

We mimic the classical construction.

Definition 5.1. Define subsets C_1 and C_2 of the set of all valuation rings of a field by

$$\begin{aligned} C_1 &:= \{\mathcal{O} : \mathcal{O} \text{ is } c\text{-henselian and } \mathcal{O}/\mathcal{M} \text{ is not } c\text{-closed}\} \\ C_2 &:= \{\mathcal{O} : \mathcal{O} \text{ is } c\text{-henselian and } \mathcal{O}/\mathcal{M} \text{ is } c\text{-closed}\}. \end{aligned}$$

If we want to emphasize the ambient field in question, we write $C_1(K)$, resp. $C_2(K)$.

Note: Since K itself is always a c-henselian valuation ring of K, the set $C_1 \cup C_2$ is never empty.

Remark 5.2. Suppose that $\mathcal{O} \subset \mathcal{O}'$ are valuation rings of K and $\mathcal{O}'$ has c-closed residue field $\mathcal{O}'/\mathcal{M}'$. Then by the Lifting Property (L), we know that the valuation ring $\mathcal{O}/\mathcal{M}'$ of $\mathcal{O}'/\mathcal{M}'$ has c-closed residue field $\mathcal{O}/\mathcal{M}$. Hence $\mathcal{O}$ also has a c-closed residue field.

Recall that two valuation rings $\mathcal{O}$ and $\mathcal{O}'$ are called 'comparable' if one is a subset of the other.

Proposition 5.3. *Any two valuation rings from C_1 are comparable. If C_2 is non-empty, then C_2 contains a valuation ring which is coarser than every valuation ring from C_2 and strictly finer than every valuation ring from C_1. If C_2 is empty, then there is a finest valuation ring in C_1.*

Proof. We first show that two rings from C_1 are always comparable. Indeed, assume $\mathcal{O}_1, \mathcal{O}_2$ are incomparable c-henselian valuations. We will show that they are both in C_2, i.e. they have c-closed residue fields. It follows from the assumed incomparability that $\mathcal{O} := \mathcal{O}_1\mathcal{O}_2$ is a proper coarsening of $\mathcal{O}_1$ and $\mathcal{O}_2$ and that the valuation rings $\mathcal{O}_1/\mathcal{M}$ and $\mathcal{O}_2/\mathcal{M}$ of $\mathcal{O}/\mathcal{M}$ are independent. Furthermore, by Lemma 4.10, they are both c-henselian. Thus by the (S)-property of $\mathcal{C}$, $\mathcal{O}/\mathcal{M}$ is c-closed. By Remark 5.2, the residue fields of $\mathcal{O}_1$ and $\mathcal{O}_2$ are also c-closed: that is, they are in C_2.

Now, if C_1 is non-empty, then since all rings in C_1 are comparable, the intersection $\mathcal{O}^* := \bigcap_{\mathcal{O}\in C_1} \mathcal{O}$ is a valuation ring with maximal ideal $\bigcup_{C_1} \mathcal{M}$, which is clearly finer than every valuation ring in C_1. By Lemma 3.5, it is easy to see that $\mathcal{O}^*$ is c-henselian, so if $C_2 = \emptyset$, then $\mathcal{O}^*$ is a finest valuation ring in C_1, proving the last claim of the proposition.

Next suppose $C_2 \neq \emptyset$. Then a simple Zorn's Lemma construction shows that C_2 has a maximal element $\mathcal{O}^{**}$. Property (S) implies this element is unique. For supposing $\mathcal{O}_1$ and $\mathcal{O}_2$ are two distinct maximal elements, then their compositum $\mathcal{O}_3 := \mathcal{O}_1\mathcal{O}_2$ is c-henselian and Kv_3 has two independent c-henselian valuation rings $\mathcal{O}_1/\mathcal{M}_3$ and $\mathcal{O}_2/\mathcal{M}_3$. Hence $\mathcal{O}_3$ is in C_2, contradicting maximality. □

Definition 5.4. The *canonical c-henselian valuation* of K, denoted by $\mathcal{O}_c$ (or v_c), is defined to be $\mathcal{O}^*$ if $C_2 = \emptyset$, and $\mathcal{O}^{**}$ otherwise. We also put

$$C := C_1 \cup \{\mathcal{O}_c\}.$$

Thus the canonical c-henselian valuation is the finest valuation ring in C. If we want to emphasize the ambient field, we write $C(K)$.

The point of this construction is that the canonical valuation enjoys many good structural properties not enjoyed by an arbitrary c-henselian valuation. The main such properties are summarized in the following

Proposition 5.5. *The canonical c-henselian valuation satisfies the following properties.*

- *$\mathcal{O}_c$ is non-trivial if and only if K is not c-closed and admits a non-trivial c-henselian valuation.*
- *If $\mathcal{O} \in C$ then $\mathcal{O}$ is comparable to any other c-henselian valuation*
- *If $\mathcal{O}_c$ does not have c-closed residue field, then neither does any other c-henselian valuation ring on K*

- *If $\mathcal{O}$ is strictly coarser than $\mathcal{O}_c$, then $\mathcal{O}/\mathcal{M}$ is not c-closed. If $\mathcal{O}$ is finer than $\mathcal{O}_c$, it has c-closed residue field.*
- *If K is c-closed, then $C = \{K\}$.*

Proof. Follows easily from the construction. For example, for the second property, since C_1 and C_2 partition the set of c-henselian valuations, and $\mathcal{O}_c$ is comparable to every element in C_1 and C_2 by construction, it is comparable to every c-henselian valuation. □

6 Three 'Going-Down' results

The formal properties of the canonical valuation are all that is required to prove the analogues of the three 'Going-Down' theorems from [1] for c-henselian valuations. We prove the two we will need later and leave the third as an exercise to the reader. The proofs follow those in [1].

Proposition 6.1. *Let $L \in \mathcal{C}(K)$ be a normal extension, and suppose $\mathcal{O}' \in C(L)$. Then $\mathcal{O} := \mathcal{O}' \cap K \in C(K)$.*

Proof. If $L = L^c$ then $\mathcal{O}' = L$ and $\mathcal{O} = K$, and the claim is trivial.

Suppose then that $L \neq L^c$ and $\mathcal{O}'$ is non-trivial. We will show that $\mathcal{O}'$ is the unique extension of $\mathcal{O}$ to L, and hence that $(K, \mathcal{O})$ is c-henselian. Indeed, let $\mathcal{O}''$ be any extension of $\mathcal{O}$ to L. Then there is some $\sigma \in Gal(L/K)$ such that $\mathcal{O}'' = \sigma(\mathcal{O}')$. Hence $\mathcal{O}''$ is also c-henselian, and so by Proposition 5.5, is comparable, and hence equal to, $\mathcal{O}'$: indeed, distinct prolongations of a valuation to an algebraic extension are never comparable, by Lemma 3.2.8 in [1].

We finally show that $\mathcal{O}_c(K) \subseteq \mathcal{O}$. Assume for a contradiction that $\mathcal{O}$ is strictly contained in $\mathcal{O}_c(K)$. By Prop 5.3, $\mathcal{O} \in C_2(K)$. Now, by standard valuation theoretic arguments, we can find an extension $\mathcal{O}'''$ of $\mathcal{O}_c(K)$ to L containing $\mathcal{O}'$: in particular, $\mathcal{O}'''$ contains $\mathcal{O}_c(L)$. In fact, it strictly contains it, since otherwise, upon restricting to K, we would get $\mathcal{O} = \mathcal{O}_c(K)$, contrary to assumption. Hence, by Prop. 1.11, $\mathcal{O}'''$ does not have c-closed residue field. Hence neither does $\mathcal{O}_c(K)$, implying $C_2(K) = \emptyset$, contradiction. □

Proposition 6.2. *Suppose L is not c-closed, and let $L \in \mathcal{C}(K)$ be a finite extension. If $\mathcal{O}' \in C(L)$, then $\mathcal{O} := \mathcal{O}' \cap K \in C(K)$.*

Proof. One first passes to the normal hull of L/K, and then proceeds as above. □

For the last Going-Down result, concerning Sylow p-extensions, we will need to add some extra technical conditions in the case $p = 2$ (see [1] page 108-109). Recall (see [1] p. 109) that if there is a c-henselian valuation with real-closed residue field, then there exists a valuation ring $\mathcal{O}^+ \in C_1(L)$ maximal with respect to the property of having a real-closed residue field.

Proposition 6.3. *Let $L \in \mathcal{C}(K)$ be a Sylow p-extension and let $\mathcal{O}' \in C(L)$. If $p = 2$ and the residue field of $\mathcal{O}'$ is real-closed, we also assume $\mathcal{O}'$ is coarser than $\mathcal{O}^+$. Then $\mathcal{O} := \mathcal{O}' \cap K \in C(K)$.*

Proof. Assume $\mathcal{O}'$ is non-trivial, so $L \neq L^c$ by Proposition 5.5. Let $\mathcal{O}^c$ be the unique extension of $\mathcal{O}'$ to L^c. Now let $M \in \mathcal{C}(L)$ be finite over L, and set $\mathcal{O}_1 = \mathcal{O}^c \cap M$, evidently a c-henselian valuation. We claim that $\mathcal{O}_1$ is the only c-henselian valuation ring of M restricting to $\mathcal{O}$.

Indeed, assume $\mathcal{O}_2$ is another such ring. Then we first claim $\mathcal{O}_1$ and $\mathcal{O}_2$ are not independent. Otherwise, $M = M^c$ by the (S) property, so $L^c = M$ is finite. By the (R) property, $[L^c : L] = 2$, and since L is the fixed field of a Sylow p-subgroup, $[M : L] = [L^c : L] = p^n$ for some n. It follows that $p = 2$ and $L^c = L(2)$, so L, and hence also its residue field with respect to $\mathcal{O}'$, is real-closed. But note that we assumed $\mathcal{O}'$ was coarser than $\mathcal{O}^+$, and so L cannot be real-closed: contradiction. Therefore $\mathcal{O}_1$ and $\mathcal{O}_2$ are not independent.

They are also incomparable, since they are distinct valuation rings both restricting to $\mathcal{O}$. Hence $\mathcal{O}_3 := \mathcal{O}_1\mathcal{O}_2$ is non-trivial, and its residue field $k := \mathcal{O}_3/\mathcal{M}_3$ has independent valuations $\mathcal{O}_1/\mathcal{M}_3$ and $\mathcal{O}_2/\mathcal{M}_3$. Note that these valuations are c-henselian by Lemma 4.10. Hence, by the (S)-property, $k = k^c$. Now since $\mathcal{O}_1$ and $\mathcal{O}_2$ are non-comparable, $\mathcal{O}_1$ is a proper subset of $\mathcal{O}_3$, implying that $\mathcal{O}_3 \cap L$ is strictly coarser than $\mathcal{O}_c(L)$. Indeed, otherwise, upon restricting both to L, we find $\mathcal{O}' = \mathcal{O}_3 \cap L$, and since the former is c-henselian, this forces $\mathcal{O}_1 = \mathcal{O}_3$, contradicting the fact that $\mathcal{O}_1$ and $\mathcal{O}_2$ are not comparable. Hence $\mathcal{O}_3 \cap L$ does not have c-closed residue field k''. Since $[M : L]$ is finite, so is $[k : k'']$, with $k = (k'')^c$. It follows from the (R)-property that the degree of the extension is 2, and so by Lemma **??**, 2 divides $[M : L]$. As L is the fixed field of a Sylow p-subgroup, $[M : L]$ must be of degree p^n for some n. This implies that $p = 2$: in this case we have assumed that $\mathcal{O}'$

is coarser than $\mathcal{O}^+$. But then $\mathcal{O}''$ is strictly coarser than $\mathcal{O}^+$ and still has real-closed residue field, which gives a contradiction.

It is now straightforward to show that $\mathcal{O}$ is c-henselian, since it has a unique extension to M, which is itself c-henselian. □

7 Rigid elements

We recall the fundamental results from the theory of so-called 'rigid elements'. This will be the key input to recover any sort of valuation whatsoever from the absolute Galois group. The theory developed above will then be used to bootstrap this valuation up to what we want.

Let $\mathcal{O}_v$ be a valuation ring of a field K. Then if $x \in K^\times \setminus \mathcal{O}_v^\times$, the ultrametric inequality implies the additive and multiplicative action of $\mathcal{O}_v^\times$ on x possesses a certain rigidity, in the sense that one can never move too far away from x. Precisely, one has

$$\mathcal{O}_v^\times + x\mathcal{O}_v^\times \subseteq \mathcal{O}_v^\times \cup x\mathcal{O}_v^\times \tag{5}$$

It turns out that any subgroup $T \leq K^\times$ which acts in a similarly rigid fashion on elements of $K^\times \setminus T$ must be induced by a valuation ring.

Definition 7.1. If $x \in K^\times \setminus T$, then we call x T-rigid if

$$T + xT \subseteq T \cup xT$$

For simplicity we restrict now to the special case where $(F^\times)^p \leq T$ for some prime p. In this case, define the sets

$$\begin{aligned} \mathcal{O}_1(T) &:= \{x \in K \setminus T : 1 + x \in T\} \\ \mathcal{O}_2(T) &:= \{x \in T : x\mathcal{O}_1(T) \subseteq \mathcal{O}_1(T)\} \end{aligned}$$

and

$$\mathcal{O}(T) := \mathcal{O}_1(T) \cup \mathcal{O}_2(T).$$

Proposition 7.2. *Given the setup as above, suppose in addition that every element in $K^\times \setminus T$ is T-rigid, and if $p = 2$, assume that $-1 \in T$. Then if $p \neq 2$, $\mathcal{O}(T)$ defines a valuation ring of K with $\mathcal{O}(T)^\times \subseteq T$. If $p = 2$, there exists a subgroup $T' \leq K^\times$ containing T such that $[T' : T] = 2$ and $\mathcal{O}(T')$ is a valuation ring of K with $\mathcal{O}(T')^\times \subseteq T'$.*

Proof. This is Theorem 2.2.7 in [1]. □

So provided $p \neq 2$, the valuation ring will be non-trivial if and only if $T \neq K^\times$.

The next lemma gives a powerful method for detecting the existence of subgroups T satisfying the criterion of proposition 7.2.

Lemma 7.3. *Let p be an odd prime, K a field. Suppose $S \leq K^\times$ is a subgroup of index $[K^\times : S] \geq p^2$, such that for any $x \in K^\times \setminus S$,*

$$S + xS \subseteq \bigcup_{i=0}^{p-1} x^i S.$$

Then there is a subgroup $T \leq K^\times$ with $S \subseteq T$, $[T : S] \leq p$, and every $x \in K^\times \setminus T$ is T-rigid.

Proof. This is Lemma 2.14 in [5]. □

For later use, we also make the following definition:

Definition 7.4. Given a field K and a prime p, an element $a \in K \setminus K^p$ is called *strongly p-rigid* iff it is $(K^\times)^p$-rigid, i.e., iff

$$K^p + aK^p \subseteq K^p \cup aK^p.$$

Proposition 7.2 shows sufficiently many strongly p-rigid elements induce the existence of a non-trivial valuation ring. In fact, in [6] it was shown, using model theory, that even just a single strongly p-rigid element already implies the existence of such a valuation.

8 A Galois-theoretic characterization of c-henselianity

A Galois theoretic characterization for a field to admit a non-trivial p-henselian valuation was obtained in [4], provided the field contains a primitive p-th root of unity ζ_p. The formal properties of canonical valuations established above allow us to obtain an analogous characterization for the existence of a c-henselian valuation in terms of the maximal $\mathcal{C}$-quotient of the absolute Galois group.

Definition 8.1. A valuation v on a field K is said to be *tamely branching* at the prime p if $char(Kv) \neq p$, $\Gamma_v \neq p\Gamma_v$. If $[\Gamma_v : p\Gamma_v] = p$, we also require that Kv is not p^2-closed, that is, there exists a separable extension of Kv of degree divisible by p^2.

Notice that if $p = 2$ and Kv is formally real, then Kv admits an extension of degree 2 but not degree 4, as $[Kv^{sep} : Kv] = 2$. This is however the only case for which having an extension of degree p does not imply that there is also an extension of degree p^2. So outside of this case, the last condition is equivalent to Kv not being p-closed.

The following observation will be crucially used later.

Lemma 8.2. *Let F be a finite extension of $\mathbb{Q}_p$. Then F does not admit any p-henselian valuation tamely branching at p.*

Proof. Let v_p denote the p-adic valuation, and suppose w is another valuation which is p-henselian tamely branching at p. As v_p is a rank 1 valuation and has a residue field which is not p-closed, w must be a refinement of v_p, and hence must have residue characteristic p: contradiction. □

We now present a sharpening of the Galois-characterization for p-henselian valuations tamely branching at p obtained in [4]. Recall Definition 3.1 of the maximal elementary $\mathbb{Z}/p\mathbb{Z}$ meta-abelian extension. Let us also recall that if $F = \mathbb{Q}_{\lessdot}(\zeta_p)$, $lnot = p$, then one can show that $G_F(p) \simeq \mathbb{Z}_p \rtimes \mathbb{Z}_p$, and so the maximal elementary $\mathbb{Z}/p$ meta-abelian quotient is $\simeq \mathbb{Z}/p^2\mathbb{Z} \rtimes \mathbb{Z}/p^2\mathbb{Z}$. For this field F it is also known that the norm maps $N_{L/F}$ are not surjective when $L = F(\sqrt[p]{a})$. By Lemma 3.3, the same will therefore be true of any other field K for which the maximal elementary $\mathbb{Z}/p$ meta-abelian quotientof G_K is of the same form.

Proposition 8.3. *Let p be a prime, and let K be a field with a primitive p-th root of unity. Let K'' denote the maximal elementary $\mathbb{Z}/p\mathbb{Z}$ meta-abelian extension of K. Then K admits a p-henselian valuation tamely branching at p whenever $Gal(K''/K) \simeq \mathbb{Z}/p^2\mathbb{Z} \rtimes \mathbb{Z}/p^2\mathbb{Z}$.*

Proof. We will only treat the case $p > 2$ in what follows. The case $p = 2$ follows using the same method as in [1] Lemma 5.4.4.

Let us suppose first of all that $G := Gal(K''/K) \simeq \mathbb{Z}/p^2\mathbb{Z} \rtimes \mathbb{Z}/p^2\mathbb{Z}$. Then by Kummer theory,

$$\dim_{\mathbb{F}_p} K^\times/(K^\times)^p = \mathrm{rank}(G) = 2.$$

Suppose $H \leq G$ is a subgroup of index p. Then we claim that $H \simeq \mathbb{Z}/p^i\mathbb{Z} \rtimes \mathbb{Z}/p^j\mathbb{Z}$ where $i, j \in \{1, 2\}$. Indeed, the embedding $H \hookrightarrow \mathbb{Z}/p^2\mathbb{Z} \rtimes \mathbb{Z}/p^2\mathbb{Z}$ induces the following commutative diagram with exact rows:

$$\begin{tikzcd}
1 \arrow[r] & \mathbb{Z}/p^2\mathbb{Z} \arrow[r, hook, "g"] & G \arrow[r, two heads, "f"] & \mathbb{Z}/p^2\mathbb{Z} \arrow[r] & 1 \\
1 \arrow[r] & H'' \arrow[r, hook] \arrow[u, hook] & H \arrow[r, two heads] \arrow[u, hook] & H' \arrow[r] \arrow[u, hook] & 1
\end{tikzcd}$$

where $H'' = im(g) \cap H$, $H' = f(H)$, and since H' is cyclic, the splitting of the top sequence induces one for the bottom one. So $H \simeq H' \rtimes H''$. If H' or H'' were trivial, then H would have index greater than p, contradicting our assumption.

If L is an extension of K of degree p, applying the above in the case when $H = Gal(K^{''}/L)$, we see that

$$\dim_{\mathbb{F}_p} L^\times/(L^\times)^p = \operatorname{rank}(H) = 2 \tag{6}$$

as well. Armed with this crucial observation, we now wish to use Lemma 7.3 with $S = (K^\times)^p$.

If we let

$$\langle x \rangle := \bigcup_{i=0}^{p-1} x^i (F^\times)^p$$

then we need to show that for every $x \in F^\times \setminus (F^\times)^p$, $(F^\times)^p + x(F^\times)^p \subset \langle x \rangle (F^\times)^p$, where this last set denotes the multiplicative group generated by x and $(F^\times)^p$. Notice that for any $a, b \in F^\times$, $z := a + \sqrt[p]{x}b \in L := K(\sqrt[p]{x})$ has norm $N_{L/F}(z) = a^p + xb^p$. Therefore the conditions of Lemma 7.3 are met if we can show that

$$N_{L/F}(L^\times) = \langle x \rangle (F^\times)^p \tag{7}$$

for any such L. Since $N_{L/F}(\sqrt[p]{x}) = x$, we have that $\langle x \rangle (F^\times)^p \subset N_{L/F}(L^\times)$ and, since $x \notin F^p$, $\sqrt[p]{x} \notin L^p$. By Lemma 3.2 and the discussion preceeding the statement we are proving, $N_{L/F} : L \to F$ is not surjective. Thus we may find $y \in F^\times \setminus \langle x \rangle (F^\times)^p$. Since $L^p \cap F = F^p$, $y \notin \langle \sqrt[p]{x} \rangle (L^\times)^p$. Thus y and $\sqrt[p]{x}$ are independent elements in the $\mathbb{F}_p$-vector space $L^\times/(L^\times)^p$, which is 2-dimensional by (2.3). Thus

$$L^\times = \langle y \rangle \langle \sqrt[p]{x} \rangle (L^\times)^p$$

from which, by taking norms, we obtain (2.4) as desired.

Since $[\Gamma : p\Gamma] = [K^\times : (K^\times)^p] = p^2$, we can use Lemma 7.3 together with Proposition 7.2 to see that K admits a valuation $\mathcal{O}$ with $\mathcal{O}^\times \leq T$, for some $T \subsetneq F^\times$ containing $(F^\times)^p$. Since then $\mathcal{O}^\times (F^\times)^p \subset T \neq F^\times$, we have $\Gamma_v \neq p\Gamma_v$.

The rest of the proof now proceeds exactly as in [4]. □

We are now ready to deduce the first main result, giving a Galois theoretic characterization for a field to admit a c-henselian valuation. We will assume in the proof that $p > 2$ for simplicity.

Theorem 8.4. *Let K be any field, and let $\mathcal{C}$ be a canonical class containing $\mathcal{C}_p$ for some prime p. If $K(\zeta_p) \notin \mathcal{C}(K)$, then we will also assume that $\zeta_p \in K$. Then there is a c-henselian valuation v on K tamely branching at p if and only if $Gal(K^c/K)$ has a non-procyclic p-Sylow subgroup with a non-trivial abelian normal subgroup.*

Proof. ("$\Rightarrow$"): If K admits such a valuation, then the valuation extends to a c-henselian valuation on the fixed field of *any* p-Sylow subgroup S of $Gal(K^c/K)$. By Hilbert ramification theory, the inertia subgroup of this extended valuation is a non-trivial normal abelian subgroup, and S is not procyclic.

("$\Leftarrow$"): Let S be such a Sylow subgroup, with fixed field F. By assumption S admits a non-trivial abelian normal subgroup $A \simeq \mathbb{Z}_p^r$ where $r = rank(A)$.

If $r > 1$, then S has a normal subgroup of the form $\mathbb{Z}_p \rtimes \mathbb{Z}_p$, and so its fixed field is a *normal* field extension L/F inside K^c such that

$$Gal(K^c/L) = Gal(L^c/L) \simeq \mathbb{Z}_p \rtimes \mathbb{Z}_p.$$

Since

$$cd_p(\mathbb{Z}_p \rtimes \mathbb{Z}_p) = 2$$

we find $char(L) \neq p$, since the p-cohomological dimension of a field of characteristic p is always ≤ 1 (see [13] Chapter 2, Section 2.2). By construction[4], $L(p) = L^c = K^c$, and $Gal(L^c/L)(p) = Gal(L(p)/L) \simeq \mathbb{Z}_p \rtimes \mathbb{Z}_p$. If $K(\zeta_p) \notin \mathcal{C}(K)$, then $\zeta_p \in K \subset L$ by assumption. On the other hand, suppose $K(\zeta_p) \in \mathcal{C}(K)$. We have that $[K(\zeta_p) : K]$ divides $p - 1$. Since $\zeta_p \in K^c$,

[4] Noting that since $\mathcal{C}$ contains $\mathcal{C}_p$, K^c is p-closed.

but there are only p-power extensions between L and K^c, it must therefore be that $\zeta_p \in L$. Thus in all cases, $\zeta_p \in L$. Then by Proposition 8.3, there is a p-henselian valuation w on L tamely branching at p. Since $L(p) = L^c$, the valuation is actually c-henselian. Let v be the canonical c-henselian valuation on L. By Proposition 5.5, v is still tamely branching at p. By Proposition 6.1, its restriction to F is again c-henselian, and clearly still has residue characteristic not p and value group not p-divisible. Finally, by Proposition 6.3, we may once more restrict to K and obtain a c-henselian valuation tamely branching at p as desired.

If $r = 1$, then since S is not pro-cyclic, there is $g \in S \setminus A$ such that

$$A \rtimes \langle g \rangle \simeq \mathbb{Z}_p \rtimes \mathbb{Z}_p.$$

Letting L be the fixed field of this semidirect product, we find in the same way as above that L has a c-henselian valuation tamely branching at p. Its unique prolongation w to the fixed field $Fix(A)$ of A has non-p-divisible value group and residue characteristic not p, and so the same will be true for w_c, the canonical c-henselian valuation on $Fix(A)$. By the 'Going-Down' results, the restriction of w_c to L is c-henselian and tamely branching, and therefore so is its restriction to F, which gives us the desired valuation. □

Remark 8.5. For example, we may take $\mathcal{C}$ to be $\mathcal{C}_{solv}$ in the above. Since $K(\zeta_p)$ is a solvable extension, we do not in this case need to assume anything about K containing ζ_p.

We record the following strengthening of the above utilizing the full sharpening obtained in Proposition 8.3.

Definition 8.6. We denote by K^{pq} the compositum of all elementary abelian $\mathbb{Z}/q\mathbb{Z}$ extensions of K'', the elementary $\mathbb{Z}/p\mathbb{Z}$ meta-abelian extension of K. We call K^{pq} the maximal (p,q)-meta-abelian extension of K.

Corollary 8.7. *Let K be any field containing ζ_p and let $\mathcal{C} = \mathcal{C}_{p,q}$, the class of all finite groups of order $p^n q^m$ for some n, m. Then there is a c-henselian valuation v on K tamely branching at p if and only if $Gal(K^{pq}/K)$ has a non-procyclic p-Sylow subgroup with a non-trivial abelian normal subgroup.*

Proof. This follows in the exact same way as the proof of the above Theorem. □

9 Recovering the p-adic valuation

Now let $\mathcal{C}$ be any canonical class containing $\mathcal{C}_{p,q}$: for example $\mathcal{C}_{p,q}$ or $\mathcal{C}_{solv}$. Thus Theorem 8.4 can be applied in this context. We will now show that if we impose extra structure on the groups in question, we are rewarded with extra structure on the valuations obtained in this way. We will first need some preliminary technical results.

Proposition 9.1. *Let (K, v) be a valued field of mixed characteristic $(0, p)$ such that $\mathcal{O}[1/p] = K$, $K^\times/(K^\times)^p$ is finite. Then Kv is perfect. If in addition $\Gamma_v \neq p\Gamma_v$, then $\Gamma_v \simeq \mathbb{Z}$ and Kv is a finite field.*

Proof. This is just [10] Lemma 2.4. □

The proof of the next proposition was related to the author by Koenigsmann.

Proposition 9.2. *Let (K, v) be a p-henselian valued field of mixed characteristic $(0, p)$ with $\mathcal{O}_v[1/p] = K$ and suppose that $G_K(p)$ is finitely generated. Then*

$$\Gamma_v = p\Gamma_v \implies cd(G_K(p)) \leq 1.$$

Proof. By Lemma 3.3, it suffices to show that for any $a \in K^\times \setminus (K^\times)^p$,

$$N_{L/K} : L^\times \to K^\times$$

is surjective, where $L = K(\sqrt[p]{a})$. Since $\Gamma_v = p\Gamma_v$, $K^\times = \mathcal{O}_v^\times (K^\times)^p$, and so a may be taken to be a unit. Since the residue characteristic is a perfect field of characteristic p by Proposition 9.1, we may further take a to be in $1 + \mathcal{M}$, say $a = 1 + y$.

Let α be a primitive element for L/K which is integral and has trace 1. Now we claim that there is $x \in K$ such that

$$N_{L/K}(1 + x\alpha) = 1 + y.$$

Indeed, expanding the norm we get $N(\alpha)x^p + \ldots - x + 1 = 1 + y$. Let $f(x) \in \mathcal{O}[x]$ be $N(\alpha)x^p + \ldots - x - y$: we need to show that f admits a root in K. But $\bar{f}(\bar{y}) = 0$ since $v(y) > 0$. This root is furthermore simple, since $f'(y) = y(ay^{p-1} + \ldots) - a$ which becomes -1 in the residue field. By p-henselianity, this root lifts to K as desired. □

In fact, it is possible to prove the following even stronger result, though we omit its proof as its full strength is not necessary for our considerations.

Proposition 9.3. *Let (K, v) be a p-henselian valued field of mixed characteristic $(0, p)$ with $\mathcal{O}_v[1/p] = K$ and suppose that $G_K(p)$ is finitely generated. Then if $\Gamma_v = p\Gamma_v$, there exists a field F of characteristic p such that $G_K(p) \simeq G_F(p)$.*

The last result we need is a strengthening of a lemma by Pop (Satz 4 of [9]). We simply optimize his original proof.

Lemma 9.4. *Let $G := Gal(F^{pq}/F) = G_F^{pq}$ where F is a finite extension of $\mathbb{Q}_p$ and F^{pq} is as in Definition 8.6. Then there is a p-subgroup R of G such that if $H \trianglelefteq G$ is non-trivial, then $H \cap R \neq \{1\}$.*

Proof. Let I_F and R_F denote the inertia and ramification subgroup of G with respect to the p-adic valuation on F. We claim that R_F satisfies the desired property.

Indeed, suppose H is any normal subgroup, and let L be the fixed field of H in F^{pq}. Then note that $R_F \cap H = R_L$, the ramification subgroup of the p-adic valuation on L. So we need to show that this ramification group is non-trivial. We will show that the p-Sylow subgroups of G_L^{pq} are non-cyclic. Assuming this, note that if $R_L = 1$, then $I_L \simeq (\mathbb{Z}/q)^r$ for some r. Also, $G_L^{pq}/I_L \simeq G_{Lv}^{pq}$. The Sylow subgroups of G_L^{pq}/I are of the form PI/I where P is a Sylow subgroup of G_L^c. Since I_L is not pro-p (and has no pro-p quotients) it commutes with any Sylow subgroup P as both are normal. Thus PI/I is cyclic if and only if P is cyclic. But $G_{Lv}^{pq} \simeq \mathbb{Z}/p \times \mathbb{Z}/q$ clearly has a cyclic p-Sylow subgroup, which gives us our desired contradiction.

Let F_1/F be any Galois sub-extension of F^{pq} not contained in L, and put $k = F_1 \cap L$, $L_1 = F_1' \cap L$, where F_1' is the maximal elementary abelian $\mathbb{Z}/p$-extension of F_1. Since L_1 and F_1 are linearly disjoint,

$$Gal(L_1/L)^c \simeq Gal(L_1F_1/F_1)^c$$

and $Gal(L_1F_1/F_1)$ is a quotient of $Gal(F_1'/F_1)$. Therefore L_1'/k is a $\mathbb{Z}/p\mathbb{Z}$-extension. Now

$$[F_1' : L_1F_1] = \frac{[F_1' : F_1]}{[L_1 : k]} \geqslant p^{a-b}$$

where $a = [F_1 : \mathbb{Q}_p], b = [k : \mathbb{Q}_p]$. By taking an element α in F^{pq} of degree p^2q over F but not contained in L, we may choose $F_1 = F(\alpha)$. Since L/F

is of degree at most p^2q, $[F_1 : k]$ is at least degree p or q, and in either case is at least 2. Then $a - b \geqslant 2$ by the Tower Law, and so $p^2 \mid [F_1^{'} : L_1F_1]$. It follows that $Gal(F_1^{'}/L_1F_1)^c$ is at least $(\mathbb{Z}/p\mathbb{Z})^2$ and so is not cyclic.

Now, any p-Sylow subgroup of $Gal(F_1^{'}/L_1)^{pq}$ must contain $Gal(F_1^{'}/L_1F_1)^{pq}$, as it's a subgroup of the p-group $Gal(F_1^{'}/F_1)^c$. Because any subgroup of a cyclic group is cyclic, it follows that $Gal(F_1^{'}/L_1)^{pq}$ has no cyclic p-Sylow subgroups. Since $Gal(F_1^{'}/L_1)^c \simeq Gal(LF_1^{'}/L)^{pq}$, neither does $Gal(LF_1^{'}/L)^{pq}$. But as this is a quotient of G_L^{pq}, it follows that G_L^{pq} also cannot have any cyclic p-Sylow subgroups. □

Armed with the above technicalities, we are ready to prove the second main result.

Theorem 9.5. *Let F a finite extension of $\mathbb{Q}_p$ containing ζ_p and ζ_q with p-adic valuation v_p. Choose $\mathcal{C}$ to be any canonical class containing $\mathcal{C}_{p,q}$, where q is any prime different from p. Suppose L is any field with*

$$G_L^c \simeq G_F^c,$$

where, if $L(\zeta_n) \notin \mathcal{C}(L)$, $n \in \{p, q\}$, we additionally assume that $\zeta_n \in L$. Then there is a c-henselian valuation v on L with Lv a finite field of characteristic p and $\Gamma_v \simeq \mathbb{Z}$. Furthermore, there is a finite extension F' of $\mathbb{Q}_p$ with p-adic valuation v_p, such that $G_{F'}^c \simeq G_F^c$, $[F' : \mathbb{Q}_p] = [F : \mathbb{Q}_p]$, and $Lv \simeq F'v_p$. If we take $\mathcal{C} = \mathcal{C}_{solv}$ then F' can be taken to be F.

Proof. Let v be the finest non-trivial c-henselian valuation on L, which exists by Theorem 8.4. Let us first show that the residue characteristic of v is p.

Suppose, for a contradiction, that the residue characteristic is not p. If $\Gamma_v \neq p\Gamma_v$ then L contains strongly p-rigid elements: indeed, it is not hard to see that any a with $v(a) \notin p\Gamma_v$ is strongly p-rigid. By the main result of [5], L therefore admits a p-henselian valuation tamely branching at p, which by Proposition 8.3 is encoded in $G_L(p)$. The isomorphism $G_L^c \simeq G_F^c$ forces their maximal pro-p quotients to be isomorphic, and since we are assuming $\mathcal{C}$ contains $\mathcal{C}_{p,q}$, these coincide naturally with the maximal pro-p quotients of the full absolute Galois group. It follows, again by Proposition 8.3, that F also admits a p-henselian valuation tamely branching at p, contradicting Lemma 8.2.

Hence it must be that $\Gamma_v = p\Gamma_v$. Because $char(Lv) \neq p$, the inertia subgroup I_v of G_L^c is normal and contains no non-trivial pro-p subgroups.

By Lemma 9.4, this forces I_v to be trivial. Hence

$$G^c_{Lv} \simeq G^c_L/I_v \simeq G^c_F.$$

Again by Theorem 8.4, Lv admits a non-trivial c-henselian valuation, from which we may obtain a proper refinement of the original valuation on L, contradicting the fact that we choose v to be the finest such. Thus it must have been the case that $\mathrm{char}(Lv) = p$.

Now, since $G_L(p) \simeq G_F(p)$ as remarked above, and $cd(G_F(p)) = 2$, Proposition 9.2 implies that $\Gamma_v \neq p\Gamma_v$. Since a p-adic field has small absolute Galois group, having only finitely many extensions of a given degree, we may apply Proposition 9.1 to deduce that $\Gamma_v \simeq \mathbb{Z}$, and that Lv is a finite field of characteristic p.

Put $L' := L \cap \overline{\mathbb{Q}}$ and let F' be the henselization of L' with respect to v', the restriction of v to L'. The induced valuation on L^h still has value group $\mathbb{Z}$ and residue field finite of characteristic p: therefore it is a finite extension of F and v' coincides with the p-adic valuation v_p. By construction,

$$G^c_{F'} \simeq G^c_L \simeq G^c_F$$

and $F'v_p \simeq Lv$. Since $G^c_{F'} \simeq G^c_F$, we have $G_{F'}(p) \simeq G_F(p)$. By [13] Section 5.6 Lemma 3, we must have that $[F' : \mathbb{Q}_p] = [F : \mathbb{Q}_p]$.

Suppose next that $\mathcal{C} = \mathcal{C}_{solv}$. Then by work of Jarden, Ritter and Jenkner ([2], [11], [3]), it follows that

$$F' \cap \mathbb{Q}_p^{ab} = F \cap \mathbb{Q}_p^{ab},$$

which forces $Lv = Fv_p$. □

Note that as before, if we take $\mathcal{C} = \mathcal{C}_{solv}$, then we do not need any extra assumptions on L containing roots of unity.

Let us also observe that from the above proof it follows that a minimal positive element in Γ_v above may be taken to be $v(\pi)$ where π is a uniformizer of F' algebraic over $\mathbb{Q}$. Indeed, the subgroup of Γ_v generated by $v(\pi)$ will already be all of $\mathbb{Z}$.

Corollary 9.6. *Let F be a finite extension of $\mathbb{Q}_p$ containing ζ_p and ζ_q. If L is any field also containing ζ_p and ζ_q, and if $Gal(L^{pq}/L) \simeq Gal(F^{pq}/F)$, then L admits a non-trivial (p,q)-henselian valuation v with $\Gamma_v \simeq \mathbb{Z}$. Furthermore, there is a finite extension F' of $\mathbb{Q}_p$ containing ζ_p and ζ_q such that $G^{pq}_{F'} \simeq G^{pq}_F$, $[F' : \mathbb{Q}_p] = [F : \mathbb{Q}_p]$ and $Lv \simeq F'v_p$.*

Proof. The proof is identical to the above, simply using Corollary 8.6. □

10 The Section Conjecture

We are now ready to prove the main result.

Theorem 10.1. *Let X be a smooth, projective variety of dimension n, where F is a finite extension of $\mathbb{Q}_p$ and F contains ζ_p and ζ_q. Then given any section s of*

$$1 \to G_{\overline{F(X)}}(p,q) \to G_{F(X)}(p,q) \to G_F(p,q) \to 1 \tag{8}$$

there exists a unique F-valuation v of $F(X)$ such that s lies above v. In particular, the existence of a section implies the existence of a point. When X is a curve, the F-valuation is induced by a unique point $a \in X(F)$ and therefore the section lies over a.

Proof. Let $s : G_F(p,q) \to G_{F(X)}(p,q)$ be a section, and let K be the fixed field in $F(X)(p)$ of $s(G_F(p,q))$. Then $G_K(p,q) \simeq s(G_F(p,q)) \simeq G_F(p,q)$. By Theorem 9.5 there is a finite extension $F'/\mathbb{Q}_p$ and a valuation v on K with value group $\mathbb{Z}$ and residue field isomorphic to $F'v_p$, where v_p is the p-adic valuation on F'. Let π be a uniformizer of F' with respect to v_p which is algebraic over $\mathbb{Q}$. Then $v(\pi)$ is a minimal positive element in Γ_v. Consider the restriction w of v to $F'(X)$. Then w still has residue field $F'v_p$ and $w(\pi)$ is still minimal positive. Let H be the subgroup of Γ_w generated by $w(\pi)$.

Since F' is complete, it admits no immediate extensions of transcendence degree n. Therefore $H \neq \Gamma_w$. Let w' be the valuation obtained from w with value group Γ_w/H. By construction, w' is trivial on F' and has residue field F', since $w'(\pi) = 0$. Since w' is a coarsening of a p-henselian valuation, it is itself p-henselian. Hence w' is an F'-valuation with $s(G_F(p)) \subset D_{w'}$.

To show uniqueness, suppose w'' is another valuation such that $s(G_{F'}(p,q)) \subset D_{w''}$. Then as both are p-henselian with residue field not p-closed, they are comparable, by Proposition 5.3 applied to the class $\mathcal{C}_{p,q}$. If w' is a coarsening of w'', then the quotient valuation w''/w' is a p-henselian valuation on an algebraic extension of F' with residue field F', and hence must be trivial. That is, $w'' = w'$. The argument is identical if w'' is a coarsening of w'. □

Corollary 10.2. *Suppose X is a smooth, projective variety over F, where F is a finite extension of $\mathbb{Q}_p$ containing ζ_p and ζ_q. Then there is a section of (8) if and only if $X(F) \neq \emptyset$.*

Proof. Note that the valuation w' of Proposition 10.1 defines an F'-rational place of $F(X)$, and hence gives rise to a point in $X(F')$. Indeed, we may always choose a generic point in $F(X)$ with positive value. Its image under the place gives a rational point $a \in X(F')$. Since the restriction map $G_K(p) \to G_F(p)$ is an isomorphism, F is relatively algebraically closed in K, and because X is defined over F, in fact $a \in X(F)$, as desired. □

Corollary 10.3. *Suppose X is a smooth, projective* curve *over F, where F is a finite extension of $\mathbb{Q}_p$ containing ζ_p and ζ_q. Then every section of (8) lies over a unique F-rational point $a \in X(F)$.*

Proof. This follows from the above corollary at once using Lemma 1.7 from [6]. Alternatively, it is a classical result that for curves, all F-valuations come from F-rational points. □

If we had used maximal solvable quotients instead of maximal (p, q)-quotients, we would obtain all the same results, except in this case no extra assumptions need to be made on the presence of roots of unity. In particular:

Corollary 10.4. *Suppose X is a smooth, projective curve over F, where F is a finite extension of $\mathbb{Q}_p$. Then every section of the exact sequence*

$$1 \to G^{solv}_{\overline{F}(X)} \to G^{solv}_{F(X)} \to G^{solv}_{F} \to 1$$

lies over a unique F-rational point.

References

[1] *A. Engler* and *A. Prestel*, Valued Fields, Springer-Verlag, 2005.

[2] *M. Jarden* and *J. Ritter*, On the characterization of the local fields by their absolute Galois groups, J. Number Th. **11** (1979), 1–13.

[3] *W. Jenkner*, Les corps p-adiques dont les groupes de Galois absolus sont isomorphes, Asterisque **209** (1992), 221–226.

[4] *J. Koenigsmann*, From p-rigid elements to valuations (with a Galois-characterization of p-adic fields), J. reine angew. Math **465** (1995), 165–182.

[5] *J. Koenigsmann*, Encoding valuations in absolute Galois groups, Fields Institute Communications **33** (2003), 107–132.

[6] *J. Koenigsmann*, On the section conjecture in anabelian geometry, J. reine angew. Math **588** (2005), 221–235.

[7] *J. Koenigsmann* and *S. K.*, Recovering valuations on Demushkin fields, Preprint (2014).

[8] *F. Kuhlmann*, *M. Pank* and *P. Roquette*, Immediate and purely wild extensions of valued fields, Manuscr. Math. **55** (1986), 39–67.

[9] *F. Pop*, Galoische Kennzeichnung p-adisch abgeschlossener Körper, J. reine angew. Math. **392** (1988), 145–175.

[10] *F. Pop*, On the birational p-adic section conjecture, Compositio Math. **146** (2010), 621–637.

[11] *J. Ritter*, p-adic fields having the same type of algebraic extensions, Ann. Math. **238** (1978), 281–288.

[12] *L. Schneps* and *P. Lochak*, Geometric Galois Actions 1, Cambridge, 1997.

[13] *J. Serre*, Galois Cohomology, Springer-Verlag, 2002.

K. Strømmen, Mathematical Institute, Oxford University, Oxford, OX2 6GG

E-mail address: `strommen@maths.ox.ac.uk`